JIM: Jurnal Ilmu Multidisiplin
E-ISSN : 2829-4580
P-ISSN : 2829-4599
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/jim.v5i2

Analisis Mengenai Serangan *Phishing* sebagai suatu Bentuk Kejahatan Dunia Maya dalam Pencurian Data Pribadi

Catrina Yuka[1], Felicia Angeline[2], Mirelle Elicia Perera[3], Shabrina Aurellia Nafisah Desuardi[4] ,Velliana Tanaya[5]
[1]Fakultas Hukum, Universitas Pelita Harapan, 01051230030@student.uph.edu
[2]Fakultas Hukum, Universitas Pelita Harapan, 01051230045@student.uph.edu
[3]Fakultas Hukum, Universitas Pelita Harapan, 01051230202@student.uph.edu
[4]Fakultas Hukum, Universitas Pelita Harapan, 01051230014@student.uph.edu
[5]Fakultas Hukum, Universitas Pelita Harapan, velliana.tanaya@uph.edu

Corresponding Author: 01051230045@student.uph.edu[2]

Abstract: *The phenomenon of cybercrime in the form of phishing has increased significantly along with the rapid development of digital technology and the growing reliance on the internet in daily activities. Phishing attacks exploit social engineering techniques to deceive victims into revealing sensitive personal information through electronic media such as emails, text messages, or fraudulent websites. This study aims to analyze the mechanisms of phishing attacks, their impacts on individuals and organizations, and the legal protection of personal data from the perspective of Indonesian law. The research employs a qualitative method using a literature review approach by collecting and analyzing various secondary sources, including scientific journals, cybersecurity reports, and official publications related to personal data protection and cybercrime. The results show that the success of phishing attacks is largely influenced by low digital literacy and limited awareness among internet users. The impacts include financial losses, identity theft, misuse of digital accounts, and a decline in public trust in electronic systems. Therefore, comprehensive prevention efforts are necessary through improving public digital literacy, strengthening technological security systems, and enforcing legal measures against cybercriminals.*

Keywords: *phishing, cybercrime, personal data, cybersecurity, legal protection*.

Abstrak: Fenomena kejahatan siber berupa *phishing* semakin meningkat seiring dengan pesatnya perkembangan teknologi digital dan tingginya penggunaan internet dalam berbagai aktivitas masyarakat. Serangan *phishing* memanfaatkan rekayasa sosial untuk menipu korban agar memberikan informasi pribadi yang bersifat sensitif melalui media elektronik seperti email, pesan singkat, atau situs web palsu. Penelitian ini bertujuan untuk menganalisis mekanisme serangan *phishing*, dampaknya terhadap individu dan organisasi, serta upaya perlindungan hukum terhadap data pribadi dalam perspektif hukum di Indonesia. Metode yang digunakan adalah penelitian kualitatif dengan pendekatan studi literatur melalui pengumpulan dan analisis berbagai sumber sekunder, seperti jurnal ilmiah, laporan keamanan siber, serta

publikasi resmi yang berkaitan dengan perlindungan data pribadi dan kejahatan siber. Hasil penelitian menunjukkan bahwa keberhasilan serangan *phishing* sangat dipengaruhi oleh rendahnya literasi digital dan tingkat kewaspadaan pengguna internet. Dampak yang ditimbulkan tidak hanya berupa kerugian finansial, tetapi juga pencurian identitas, penyalahgunaan akun digital, serta menurunnya kepercayaan masyarakat terhadap sistem elektronik. Oleh karena itu, diperlukan upaya pencegahan yang komprehensif melalui peningkatan literasi digital masyarakat, penguatan sistem keamanan teknologi, serta penegakan hukum yang efektif terhadap pelaku kejahatan siber.

Kata Kunci: *phishing*, kejahatan siber, data pribadi, keamanan siber, perlindungan hukum.

PENDAHULUAN

Di era digital yang semakin terintegrasi dengan kehidupan sehari-hari, data pribadi telah menjadi salah satu aset paling berharga bagi setiap individu. Informasi seperti identitas diri, nomor telepon, alamat email, data perbankan, hingga aktivitas di media sosial membentuk identitas digital seseorang di ruang siber. Semakin berkembangnya teknologi informasi dan komunikasi membuat data tersebut semakin mudah disimpan, diproses, dan dipertukarkan melalui berbagai platform digital. Namun di sisi lain, kondisi ini juga membuka peluang bagi pihak-pihak yang tidak bertanggung jawab untuk memanfaatkan data tersebut demi kepentingan yang merugikan orang lain. Salah satu bentuk kejahatan siber yang paling banyak terjadi dan terus berkembang adalah *phishing*. *Phishing* merupakan tindakan penipuan yang dilakukan dengan cara menyamar sebagai pihak atau institusi yang dianggap tepercaya oleh korban. Pelaku biasanya memanfaatkan berbagai media komunikasi elektronik seperti email, pesan singkat, aplikasi percakapan, atau situs web palsu untuk meyakinkan korban agar memberikan informasi pribadi yang bersifat rahasia. Informasi tersebut dapat berupa kata sandi akun, nomor kartu kredit, kode verifikasi, hingga data identitas yang sangat sensitif (Arif et al., 2024).

Metode *phishing* umumnya tidak hanya mengandalkan teknologi, tetapi juga memanfaatkan kelemahan psikologis manusia melalui teknik manipulasi sosial atau social engineering. Pelaku sering kali membuat pesan yang seolah-olah mendesak atau penting, misalnya pemberitahuan bahwa akun korban akan diblokir jika tidak segera melakukan verifikasi data. Dalam kondisi seperti ini, korban sering kali panik dan tidak sempat memeriksa kebenaran informasi yang diterima, sehingga tanpa sadar memberikan data pribadi kepada pihak yang sebenarnya merupakan penipu. Fenomena *phishing* semakin meningkat seiring dengan pesatnya pertumbuhan penggunaan internet di berbagai sektor kehidupan. Perkembangan teknologi digital, terutama setelah pandemi COVID-19, telah mendorong masyarakat untuk lebih banyak melakukan aktivitas secara daring. Berbagai layanan seperti transaksi perbankan, belanja online, layanan publik, hingga komunikasi sosial kini banyak dilakukan melalui platform digital. Meskipun memberikan kemudahan dan efisiensi, situasi ini juga memperluas ruang gerak bagi pelaku kejahatan siber untuk melancarkan berbagai modus penipuan.

Dampak dari serangan *phishing* tidak hanya terbatas pada kerugian finansial yang dialami korban. Dalam banyak kasus, data pribadi yang berhasil dicuri dapat digunakan untuk melakukan berbagai tindakan kejahatan lain seperti pencurian identitas, pemalsuan akun, hingga pemerasan. Selain itu, korban juga dapat mengalami kerugian secara sosial maupun psikologis, terutama apabila data yang disalahgunakan berkaitan dengan reputasi atau informasi pribadi yang bersifat sensitif. Selain merugikan individu, maraknya kasus *phishing* juga dapat memengaruhi tingkat kepercayaan masyarakat terhadap sistem digital secara keseluruhan. Ketika masyarakat merasa bahwa data mereka tidak aman, kepercayaan terhadap layanan digital seperti perbankan elektronik, perdagangan daring, maupun layanan

pemerintahan berbasis elektronik dapat menurun. Hal ini tentu menjadi tantangan serius bagi upaya pengembangan ekosistem ekonomi digital yang saat ini tengah berkembang pesat di Indonesia (Butarbutar, 2023).

Untuk menghadapi ancaman tersebut, negara telah menyediakan berbagai instrumen hukum yang bertujuan memberikan perlindungan kepada masyarakat. Salah satu regulasi yang relevan adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur berbagai aktivitas di ruang siber, termasuk tindakan penipuan dan penyalahgunaan sistem elektronik. Selain itu, pemerintah juga telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang secara khusus mengatur hak individu atas data pribadinya serta tanggung jawab pihak yang mengelola data tersebut. Keberadaan regulasi tersebut menunjukkan bahwa negara memiliki komitmen untuk melindungi masyarakat dari ancaman kejahatan siber, termasuk *phishing*. Namun demikian, perlindungan hukum saja tidak cukup untuk sepenuhnya mencegah terjadinya kejahatan ini. Kesadaran dan literasi digital masyarakat juga menjadi faktor yang sangat penting. Dengan memahami berbagai modus penipuan yang berkembang di dunia digital, masyarakat diharapkan dapat lebih waspada dalam menjaga data pribadi dan tidak mudah tertipu oleh berbagai bentuk komunikasi elektronik yang mencurigakan (Gumay et al., 2024).

Tujuan penelitian ini adalah untuk menganalisis fenomena kejahatan siber berupa *phishing*, khususnya terkait dengan mekanisme terjadinya, dampak yang ditimbulkan terhadap korban, serta bagaimana upaya perlindungan hukum terhadap data pribadi dapat diterapkan melalui peraturan perundang-undangan yang berlaku. Penelitian ini juga bertujuan untuk meningkatkan pemahaman mengenai pentingnya perlindungan data pribadi di tengah pesatnya perkembangan teknologi digital. Adapun urgensi penelitian ini terletak pada semakin meningkatnya kasus pencurian data pribadi melalui *phishing* yang dapat menimbulkan kerugian finansial, penyalahgunaan identitas, serta berbagai bentuk kejahatan lanjutan lainnya. Oleh karena itu, kajian mengenai *phishing* menjadi krusial untuk memberikan pemahaman yang lebih komprehensif kepada masyarakat sekaligus mendorong efektivitas penerapan regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam melindungi keamanan data pribadi di era digital.

METODE

Metode penelitian dalam kajian ini menggunakan jenis penelitian kualitatif dengan pendekatan studi literatur atau tinjauan pustaka. Pendekatan ini dipilih karena penelitian berfokus pada pengkajian konsep, teori, serta berbagai temuan yang telah dipublikasikan sebelumnya mengenai fenomena *phishing* dan perlindungan data pribadi. Dalam penelitian berbasis literatur, yang menjadi objek kajian bukanlah responden secara langsung, melainkan berbagai sumber informasi yang relevan seperti buku, jurnal ilmiah, laporan penelitian, serta dokumen resmi yang berkaitan dengan topik yang diteliti.

Subjek penelitian dalam kajian ini berupa berbagai sumber sekunder yang memiliki kredibilitas dan relevansi dengan isu keamanan siber, khususnya *phishing* dan perlindungan data pribadi. Sumber-sumber tersebut meliputi jurnal ilmiah yang membahas tentang kejahatan siber dan perilaku korban, laporan dari perusahaan keamanan siber, artikel berita dari media massa terpercaya yang melaporkan kasus *phishing*, serta publikasi resmi dari lembaga pemerintah yang menangani perlindungan data pribadi dan kejahatan siber. Penelitian ini tidak menggunakan sampel maupun populasi dalam arti kuantitatif, karena fokus penelitian adalah pada analisis literatur yang tersedia.

Prosedur penelitian dilakukan melalui beberapa tahapan, yaitu pengumpulan data, seleksi sumber yang relevan, pengelompokan informasi berdasarkan tema, serta analisis terhadap data yang diperoleh. Teknik analisis yang digunakan adalah teknik analisis deskriptif kualitatif, yaitu dengan menafsirkan dan menguraikan berbagai informasi yang ditemukan dalam sumber-

sumber literatur secara sistematis. Melalui tahapan tersebut, penelitian ini bertujuan untuk memberikan gambaran yang komprehensif mengenai fenomena *phishing*, taktik yang digunakan oleh pelaku, serta implikasinya terhadap perlindungan data pribadi dalam perspektif hukum di Indonesia (Yunita, 2023).

HASIL DAN PEMBAHASAN

Anatomi Serangan Phishing: Modus dan Teknik

Serangan *phishing* pada dasarnya merupakan bentuk kejahatan siber yang memanfaatkan manipulasi psikologis untuk mendapatkan informasi sensitif dari korban. Pelaku biasanya menyamar sebagai pihak yang dianggap memiliki otoritas atau kredibilitas tinggi, seperti bank, perusahaan teknologi, atau lembaga pemerintah. Dengan memanfaatkan identitas palsu tersebut, pelaku berusaha meyakinkan korban agar percaya bahwa komunikasi yang diterima adalah resmi dan sah. Strategi ini sangat efektif karena sebagian besar pengguna internet cenderung mempercayai pesan yang tampak berasal dari institusi yang dikenal. Akibatnya, korban sering kali tidak menyadari bahwa mereka sedang menjadi target penipuan. Salah satu teknik utama yang digunakan dalam *phishing* adalah rekayasa sosial atau social engineering. Teknik ini tidak bergantung sepenuhnya pada kecanggihan teknologi, melainkan pada kemampuan pelaku dalam memahami perilaku dan emosi manusia. Pelaku biasanya menciptakan situasi yang memicu rasa takut, panik, atau rasa urgensi pada korban. Misalnya, korban menerima pesan yang menyatakan bahwa rekening bank mereka akan diblokir jika tidak segera melakukan verifikasi data. Dalam kondisi panik, korban cenderung bertindak tanpa memeriksa kebenaran informasi yang diterima (Anjheli, 2024).

Selain menciptakan rasa urgensi, pelaku *phishing* juga sering memanfaatkan unsur kepercayaan. Mereka dapat menggunakan logo resmi, desain email yang menyerupai komunikasi resmi perusahaan, serta bahasa yang tampak profesional. Bahkan dalam beberapa kasus, pelaku juga menggunakan alamat email yang hampir identik dengan alamat resmi suatu organisasi. Perbedaan kecil seperti satu huruf yang diubah sering kali tidak disadari oleh korban. Hal ini membuat pesan *phishing* terlihat sangat meyakinkan bagi pengguna yang kurang teliti. Perkembangan teknologi juga membuat teknik *phishing* menjadi semakin canggih. Salah satu bentuk yang sering digunakan adalah *spear phishing*, yaitu serangan yang ditargetkan secara khusus kepada individu atau organisasi tertentu. Dalam metode ini, pelaku biasanya telah mengumpulkan informasi mengenai targetnya terlebih dahulu, misalnya melalui media sosial atau sumber informasi publik lainnya. Informasi tersebut kemudian digunakan untuk membuat pesan yang dipersonalisasi sehingga tampak lebih meyakinkan. Dengan pendekatan ini, kemungkinan korban untuk mempercayai pesan tersebut menjadi lebih besar.

Selain *spear phishing*, terdapat pula teknik yang dikenal sebagai whaling. Teknik ini secara khusus menargetkan individu dengan posisi strategis dalam organisasi, seperti direktur, manajer, atau eksekutif perusahaan. Tujuan dari serangan ini biasanya adalah untuk memperoleh akses ke sistem perusahaan atau melakukan penipuan finansial dalam jumlah besar. Karena posisi mereka yang memiliki akses luas terhadap informasi dan sistem internal, keberhasilan serangan terhadap eksekutif dapat menimbulkan dampak yang sangat serius bagi organisasi. Media yang digunakan untuk melakukan *phishing* juga semakin beragam. Jika pada awalnya *phishing* lebih banyak dilakukan melalui email, kini pelaku juga menggunakan pesan singkat atau SMS yang dikenal sebagai *smishing*. Selain itu, ada pula metode *vishing*, yaitu *phishing* yang dilakukan melalui panggilan telepon. Dalam metode ini, pelaku biasanya menyamar sebagai petugas layanan pelanggan atau perwakilan bank yang meminta korban untuk memberikan informasi pribadi. Teknik ini sering kali berhasil karena korban merasa sedang berbicara langsung dengan pihak yang berwenang (Nababan & Sumardiana, 2024).

Elemen lain dalam serangan *phishing* adalah penggunaan situs web palsu yang menyerupai situs asli. Pelaku biasanya membuat halaman web yang memiliki tampilan hampir identik dengan situs resmi suatu lembaga. Logo, tata letak, hingga warna situs dibuat semirip

mungkin dengan aslinya agar korban tidak curiga. Ketika korban memasukkan informasi seperti username, password, atau nomor kartu kredit, data tersebut langsung dikirimkan kepada pelaku. Dalam banyak kasus, korban baru menyadari penipuan tersebut setelah mengalami kerugian. Dari perspektif hukum di Indonesia, tindakan *phishing* merupakan pelanggaran serius terhadap peraturan perundang-undangan yang berlaku. Dalam Undang-Undang Informasi dan Transaksi Elektronik, tindakan penyebaran informasi yang menyesatkan dan merugikan konsumen dalam transaksi elektronik dapat dikenakan sanksi sebagaimana diatur dalam Pasal 28 ayat (1). Selain itu, akses tanpa izin terhadap sistem elektronik orang lain juga dapat dijerat dengan Pasal 30 UU ITE. Apabila tindakan tersebut melibatkan pencurian data pribadi, maka pelaku juga dapat dikenakan sanksi berdasarkan Undang-Undang Perlindungan Data Pribadi, khususnya terkait larangan memperoleh atau mengumpulkan data pribadi secara melawan hukum (Trianurahmah et al., 2024).

Kerentanan Manusia sebagai Titik Lemah Utama

Dalam sistem keamanan siber modern, teknologi perlindungan data telah berkembang sangat pesat. Berbagai perusahaan dan organisasi telah menggunakan sistem keamanan berlapis seperti enkripsi data, *firewall*, serta autentikasi dua faktor untuk melindungi informasi sensitif. Namun demikian, meskipun teknologi tersebut semakin canggih, faktor manusia tetap menjadi salah satu titik lemah utama dalam sistem keamanan digital. Banyak serangan siber berhasil bukan karena kelemahan teknologi, melainkan karena kesalahan atau kelalaian manusia dalam menggunakan sistem tersebut. Kerentanan manusia dalam menghadapi serangan *phishing* umumnya berkaitan dengan rendahnya tingkat literasi digital. Tidak semua pengguna internet memiliki pemahaman yang memadai mengenai cara kerja ancaman siber. Sebagian besar pengguna hanya menggunakan teknologi sebagai alat untuk berkomunikasi atau melakukan transaksi tanpa memahami risiko keamanan yang mungkin muncul. Kondisi ini membuat mereka lebih mudah menjadi korban berbagai bentuk penipuan digital (Yoro, 2023a).

Selain kurangnya literasi digital, faktor psikologis berperan dalam keberhasilan serangan *phishing*. Pelaku biasanya memanfaatkan emosi manusia seperti rasa takut, rasa ingin tahu, atau keinginan untuk memperoleh keuntungan. Misalnya, korban dapat menerima pesan yang menawarkan hadiah atau promosi tertentu yang tampak menarik. Tanpa memeriksa kebenaran informasi tersebut, korban mungkin langsung mengklik tautan yang diberikan dan tanpa sadar menyerahkan data pribadinya kepada pelaku. Faktor lain yang menyebabkan manusia menjadi titik lemah adalah kebiasaan pengguna dalam mengabaikan tanda-tanda peringatan keamanan. Banyak pengguna yang tidak memeriksa alamat situs web secara teliti sebelum memasukkan data pribadi. Mereka juga sering mengabaikan notifikasi keamanan yang muncul di perangkat mereka. Kebiasaan ini membuat pelaku *phishing* memiliki peluang lebih besar untuk menipu korban melalui berbagai teknik manipulasi (Bhakti, 2025).

Di lingkungan organisasi, kerentanan manusia juga dapat muncul akibat kurangnya pelatihan keamanan siber bagi karyawan. Banyak perusahaan yang fokus pada investasi teknologi keamanan tetapi tidak memberikan edukasi yang memadai kepada pegawainya. Padahal, karyawan sering menjadi pintu masuk bagi serangan siber melalui email *phishing* atau tautan berbahaya. Jika seorang karyawan tanpa sadar memberikan akses kepada pelaku, maka seluruh sistem perusahaan dapat terancam. Selain itu, perkembangan teknologi komunikasi yang sangat cepat juga membuat pengguna semakin rentan terhadap berbagai bentuk manipulasi digital. Aplikasi pesan instan, media sosial, dan platform komunikasi lainnya memungkinkan pelaku untuk menjangkau korban dengan sangat mudah. Pesan *phishing* dapat disebarkan secara massal dalam waktu singkat kepada ribuan bahkan jutaan pengguna internet. Dengan jumlah target yang besar, kemungkinan keberhasilan serangan juga meningkat.

Kerentanan manusia ini menjadi alasan penting mengapa perlindungan terhadap data pribadi tidak dapat sepenuhnya diserahkan kepada individu. Negara memiliki peran dalam

menciptakan regulasi yang dapat melindungi masyarakat dari berbagai bentuk penyalahgunaan data. Regulasi tersebut juga bertujuan untuk memastikan bahwa pihak yang mengelola data pribadi memiliki tanggung jawab dalam menjaga keamanan informasi yang mereka proses. Dalam hukum Indonesia, Undang-Undang Perlindungan Data Pribadi memberikan jaminan bahwa setiap individu memiliki hak atas keamanan data pribadinya. Salah satu ketentuan dalam regulasi ini adalah kewajiban bagi pengendali data untuk melindungi data yang mereka kelola. Ketentuan ini secara tidak langsung mengakui bahwa manusia memiliki keterbatasan dalam menjaga keamanan data. Oleh karena itu, tanggung jawab perlindungan data juga harus didukung oleh sistem keamanan yang kuat dari organisasi atau penyedia layanan digital (Yoro, 2023b).

Dampak Pencurian Data Pribadi bagi Individu

Pencurian data pribadi melalui serangan *phishing* dapat menimbulkan dampak yang sangat serius bagi individu. Data pribadi pada dasarnya merupakan bagian dari identitas seseorang yang bersifat sensitif dan tidak seharusnya diakses oleh pihak lain tanpa izin. Ketika data tersebut jatuh ke tangan yang salah, individu dapat kehilangan kendali atas informasi pribadinya. Hal ini membuka peluang bagi pelaku kejahatan untuk menyalahgunakan data tersebut dalam berbagai bentuk aktivitas ilegal. Akibatnya, korban tidak hanya mengalami kerugian materi, tetapi juga kehilangan rasa aman dalam kehidupan digitalnya. Salah satu dampak paling nyata dari pencurian data pribadi adalah kerugian finansial. Pelaku yang berhasil memperoleh informasi perbankan korban dapat melakukan transaksi tanpa izin, seperti mentransfer dana dari rekening korban atau menggunakan kartu kredit secara tidak sah. Dalam beberapa kasus, pelaku bahkan dapat menguras seluruh saldo rekening korban dalam waktu singkat. Kerugian finansial ini sering kali sulit untuk dipulihkan, terutama jika korban tidak segera menyadari bahwa akun mereka telah disusupi (Alsubaei & Almazroi, 2024).

Selain kerugian finansial langsung, data pribadi yang dicuri juga dapat digunakan untuk melakukan pencurian identitas atau *identity theft*. Dalam praktik ini, pelaku menggunakan identitas korban untuk melakukan berbagai aktivitas seperti membuka rekening bank baru, mendaftarkan layanan digital, atau mengajukan pinjaman online. Korban sering kali baru mengetahui hal tersebut ketika menerima tagihan atau tuntutan pembayaran atas transaksi yang sebenarnya tidak pernah mereka lakukan. Situasi ini tentu sangat merugikan dan dapat menimbulkan masalah hukum bagi korban. Dampak lainnya adalah hilangnya kendali terhadap akun digital pribadi, seperti akun media sosial atau email. Pelaku yang berhasil mengakses akun tersebut dapat menggunakannya untuk menyebarkan informasi palsu, melakukan penipuan kepada kontak korban, atau bahkan menyebarkan konten yang merusak reputasi korban. Dalam banyak kasus, korban juga mengalami kesulitan untuk memulihkan akun mereka karena pelaku telah mengubah kata sandi atau informasi pemulihan akun. Hal ini dapat menyebabkan gangguan serius terhadap kehidupan sosial dan profesional korban.

Pencurian data pribadi dapat menimbulkan dampak psikologis yang tidak kecil. Korban sering mengalami stres, kecemasan, dan rasa tidak aman setelah mengetahui bahwa informasi pribadi mereka telah disalahgunakan. Mereka mungkin merasa terus-menerus diawasi atau khawatir bahwa data mereka akan digunakan kembali untuk tujuan yang merugikan. Kondisi ini dapat memengaruhi kesehatan mental korban serta menurunkan rasa percaya diri dalam menggunakan teknologi digital. Selain itu, korban juga harus menghadapi berbagai proses administratif yang cukup rumit untuk memulihkan kondisi mereka. Misalnya, korban perlu melaporkan kejadian tersebut kepada pihak bank, penyedia layanan digital, atau bahkan aparat penegak hukum. Proses ini sering kali memakan waktu dan tenaga yang tidak sedikit. Dalam beberapa kasus, korban juga harus membuktikan bahwa mereka tidak terlibat dalam aktivitas ilegal yang dilakukan oleh pelaku menggunakan identitas mereka (Aditya & Yudiantara, 2025).

Dampak jangka panjang dari pencurian data pribadi juga dapat memengaruhi reputasi seseorang. Jika data yang disalahgunakan berkaitan dengan identitas atau aktivitas profesional

korban, reputasi mereka di lingkungan kerja atau masyarakat dapat terpengaruh. Misalnya, jika akun media sosial korban digunakan untuk menyebarkan konten yang tidak pantas, orang lain mungkin akan menganggap bahwa konten tersebut benar-benar berasal dari korban. Hal ini tentu dapat merusak citra dan hubungan sosial korban. Dalam kerangka hukum Indonesia, korban pencurian data pribadi memiliki hak untuk memperoleh perlindungan dan keadilan. Undang-Undang Perlindungan Data Pribadi memberikan hak kepada individu untuk menuntut ganti rugi atas kerugian yang mereka alami akibat penyalahgunaan data pribadi. Ketentuan ini memberikan dasar hukum bagi korban untuk memperjuangkan haknya melalui jalur hukum. Selain itu, pelaku yang menggunakan data pribadi secara ilegal juga dapat dikenakan sanksi pidana sesuai dengan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (Souhoka et al., 2025).

Dampak *Phishing* bagi Organisasi dan Korporasi

Serangan *phishing* tidak hanya merugikan individu, tetapi juga dapat memberikan dampak yang sangat besar bagi organisasi dan korporasi. Dalam lingkungan bisnis modern yang sangat bergantung pada teknologi digital, data merupakan salah satu aset paling berharga bagi perusahaan. Data pelanggan, informasi transaksi, serta sistem operasional perusahaan semuanya tersimpan dalam sistem elektronik. Ketika serangan *phishing* berhasil menembus pertahanan organisasi, konsekuensinya dapat sangat serius bagi keberlangsungan bisnis tersebut. Salah satu dampak utama bagi organisasi adalah kebocoran data pelanggan. Jika pelaku berhasil memperoleh akses ke sistem perusahaan melalui akun karyawan yang terkena *phishing*, mereka dapat mencuri berbagai informasi sensitif milik pelanggan. Data seperti nama, alamat, nomor telepon, hingga informasi keuangan dapat jatuh ke tangan pihak yang tidak bertanggung jawab. Kebocoran data semacam ini tidak hanya merugikan pelanggan, tetapi juga merusak reputasi perusahaan yang bertanggung jawab atas keamanan data tersebut (Reyhan & Gultom, 2025).

Selain kerugian reputasi, perusahaan juga dapat menghadapi tuntutan hukum dari pelanggan yang merasa dirugikan akibat kebocoran data. Dalam era perlindungan data yang semakin ketat, organisasi memiliki kewajiban hukum untuk menjaga keamanan data yang mereka kelola. Jika perusahaan dianggap lalai dalam melindungi data pelanggan, maka mereka dapat diminta untuk memberikan kompensasi atau ganti rugi. Proses hukum semacam ini tentu dapat menimbulkan kerugian finansial yang besar bagi perusahaan. Serangan *phishing* juga sering menjadi pintu masuk bagi serangan siber yang lebih besar dan lebih berbahaya. Misalnya, setelah memperoleh akses awal ke sistem perusahaan, pelaku dapat memasang perangkat lunak berbahaya seperti *ransomware*. *Ransomware* dapat mengenkripsi seluruh data perusahaan sehingga tidak dapat diakses oleh pihak internal. Pelaku kemudian meminta tebusan agar data tersebut dapat dipulihkan. Situasi ini dapat melumpuhkan operasional perusahaan dalam waktu yang cukup lama (Nyasvisvo & Chigada, 2023).

Selain itu, perusahaan juga harus mengeluarkan biaya yang besar untuk memulihkan sistem mereka setelah terjadi serangan siber. Biaya tersebut dapat mencakup investigasi keamanan, pemulihan data, peningkatan sistem keamanan, serta konsultasi dengan ahli keamanan siber. Tidak jarang perusahaan juga harus menghentikan sementara operasional mereka selama proses pemulihan berlangsung. Hal ini tentu berdampak langsung pada produktivitas dan pendapatan perusahaan. Dampak lain adalah hilangnya kepercayaan konsumen. Dalam dunia bisnis, kepercayaan merupakan faktor yang sangat diperlukan dalam menjaga loyalitas pelanggan. Ketika pelanggan mengetahui bahwa data mereka pernah bocor akibat serangan siber, mereka mungkin akan kehilangan kepercayaan terhadap perusahaan tersebut. Akibatnya, pelanggan dapat memilih untuk berpindah ke layanan lain yang dianggap lebih aman (Nguyen, 2023).

Dalam jangka panjang, serangan *phishing* yang berhasil juga dapat memengaruhi nilai pasar suatu perusahaan. Perusahaan yang mengalami kebocoran data besar sering kali

mengalami penurunan nilai saham karena investor merasa khawatir terhadap kemampuan perusahaan dalam mengelola risiko keamanan. Selain itu, citra perusahaan di mata publik juga dapat menurun secara signifikan. Proses pemulihan reputasi ini biasanya membutuhkan waktu yang cukup lama. Dalam hukum Indonesia, perusahaan memiliki tanggung jawab untuk menjaga kerahasiaan dan keamanan data pribadi yang mereka kelola. Undang-Undang Perlindungan Data Pribadi mengatur bahwa pengendali data wajib melindungi data pribadi dari akses yang tidak sah. Jika terjadi kebocoran data akibat kelalaian organisasi, maka perusahaan dapat dikenakan sanksi administratif hingga pidana. Ketentuan ini bertujuan untuk memastikan bahwa organisasi memiliki komitmen yang serius dalam menjaga keamanan data pelanggan (Atara et al., 2025).

Tren dan Evolusi Serangan *Phishing* di Indonesia

Dalam beberapa tahun terakhir, tren serangan *phishing* di Indonesia menunjukkan peningkatan yang cukup signifikan. Pertumbuhan jumlah pengguna internet yang sangat pesat menjadi salah satu faktor utama yang mendorong meningkatnya kasus kejahatan siber. Semakin banyak masyarakat yang menggunakan layanan digital seperti perbankan online, *e-commerce*, dan media sosial. Kondisi ini memberikan peluang yang lebih besar bagi pelaku kejahatan untuk menargetkan pengguna internet dalam skala yang luas. Pelaku *phishing* di Indonesia sering kali menargetkan layanan keuangan digital, terutama layanan perbankan dan dompet elektronik. Hal ini disebabkan karena layanan tersebut berkaitan langsung dengan transaksi keuangan yang bernilai tinggi. Pelaku biasanya mengirimkan pesan yang mengatasnamakan bank atau penyedia layanan keuangan tertentu. Pesan tersebut sering kali berisi permintaan verifikasi akun atau pemberitahuan mengenai aktivitas mencurigakan pada rekening korban (Syah, 2023).

Selain sektor perbankan, platform *e-commerce* juga menjadi sasaran utama serangan *phishing*. Banyak pengguna yang menerima pesan palsu yang mengatasnamakan toko online atau marketplace tertentu. Pesan tersebut biasanya berisi informasi mengenai promo khusus, hadiah undian, atau pemberitahuan pengiriman barang. Dengan memanfaatkan ketertarikan konsumen terhadap promo atau diskon, pelaku dapat dengan mudah menarik perhatian korban untuk mengklik tautan berbahaya. Pelaku *phishing* juga sering memanfaatkan momen-momen tertentu untuk melancarkan aksinya. Misalnya, pada saat berlangsungnya acara belanja besar seperti Hari Belanja Online Nasional atau promosi akhir tahun. Pada periode tersebut, masyarakat biasanya lebih aktif melakukan transaksi online. Pelaku memanfaatkan situasi ini dengan mengirimkan pesan yang berkaitan dengan promo atau diskon besar agar korban lebih mudah tertipu.

Seiring perkembangan waktu, teknik *phishing* di Indonesia juga semakin canggih dan terlokalisasi. Pelaku kini menggunakan bahasa Indonesia yang baik dan benar dalam pesan yang mereka kirimkan. Bahkan dalam beberapa kasus, mereka juga menggunakan istilah atau gaya bahasa yang sesuai dengan konteks budaya lokal. Hal ini membuat pesan *phishing* terlihat lebih meyakinkan dan sulit dibedakan dari komunikasi resmi. Selain melalui email, serangan *phishing* di Indonesia juga semakin banyak dilakukan melalui aplikasi pesan instan dan media sosial. Platform seperti WhatsApp dan Telegram sering digunakan oleh pelaku untuk menyebarkan tautan berbahaya. Pesan tersebut dapat disebarkan secara massal kepada banyak pengguna dalam waktu singkat. Dengan metode ini, pelaku dapat menjangkau target yang sangat luas tanpa memerlukan biaya yang besar.

Perkembangan teknologi memungkinkan pelaku untuk menggunakan teknik otomatisasi dalam menyebarkan serangan *phishing*. Misalnya dengan menggunakan bot atau sistem otomatis yang dapat mengirimkan ribuan pesan dalam waktu singkat. Teknik ini membuat serangan *phishing* menjadi semakin sulit untuk dikendalikan. Oleh karena itu, diperlukan upaya yang lebih serius dari berbagai pihak untuk mengatasi masalah ini. Dalam penegakan hukum, meningkatnya kasus *phishing* di Indonesia menuntut respons yang lebih

cepat dan efektif dari aparat penegak hukum. Undang-Undang Informasi dan Transaksi Elektronik memberikan dasar hukum bagi aparat untuk menindak pelaku kejahatan siber. Selain itu, kewenangan khusus juga diberikan kepada penyidik untuk melakukan investigasi terhadap sistem elektronik yang digunakan dalam tindak pidana. Upaya penegakan hukum ini sangat dibutuhkan untuk memberikan efek jera kepada para pelaku (Dinesh et al., 2023).

Upaya Pencegahan dan Penanggulangan

Upaya pencegahan dan penanggulangan terhadap serangan *phishing* memerlukan pendekatan yang komprehensif dan melibatkan berbagai pihak. Tidak ada satu solusi tunggal yang dapat sepenuhnya menghilangkan ancaman *phishing*. Oleh karena itu, strategi yang efektif harus mencakup kombinasi antara teknologi, edukasi, serta penegakan hukum yang kuat. Pendekatan yang terpadu ini diharapkan dapat mengurangi risiko serangan *phishing* secara signifikan. Dari sisi teknologi, penggunaan sistem keamanan yang kuat merupakan langkah dalam mencegah serangan *phishing*. Perangkat lunak keamanan seperti antivirus dan sistem deteksi spam dapat membantu mengidentifikasi pesan berbahaya sebelum mencapai pengguna. Selain itu, penggunaan autentikasi dua faktor juga dapat memberikan lapisan perlindungan tambahan terhadap akun digital. Dengan sistem ini, pelaku tidak dapat dengan mudah mengakses akun korban meskipun mereka berhasil memperoleh kata sandi (Baballe et al., 2022).

Selain teknologi, peningkatan kesadaran dan literasi digital masyarakat juga sangat diperlukan dalam mencegah *phishing*. Pengguna internet perlu memahami cara mengenali ciri-ciri pesan *phishing*, seperti tautan mencurigakan atau permintaan data pribadi yang tidak wajar. Edukasi mengenai keamanan siber sebaiknya dilakukan secara berkelanjutan melalui berbagai program sosialisasi. Dengan pemahaman yang lebih baik, masyarakat dapat menjadi lebih waspada terhadap berbagai bentuk penipuan digital. Organisasi dan perusahaan juga berperan dalam melindungi karyawan dan pelanggan mereka dari serangan *phishing*. Salah satu langkah yang dapat dilakukan adalah memberikan pelatihan keamanan siber secara berkala kepada seluruh karyawan. Pelatihan ini dapat membantu karyawan memahami berbagai teknik penipuan yang sering digunakan oleh pelaku. Sehingga, karyawan dapat menjadi garis pertahanan pertama dalam mencegah serangan siber.

Pemerintah memiliki tanggung jawab besar dalam menciptakan lingkungan digital yang aman bagi masyarakat. Hal ini dapat dilakukan melalui penyusunan regulasi yang kuat serta penegakan hukum yang tegas terhadap pelaku kejahatan siber. Selain itu, pemerintah juga dapat bekerja sama dengan berbagai pihak, termasuk perusahaan teknologi dan lembaga pendidikan, untuk meningkatkan kesadaran masyarakat mengenai pentingnya keamanan data pribadi. Kerja sama antara sektor publik dan sektor swasta juga sangat dibutuhkan dalam menghadapi ancaman *phishing*. Banyak perusahaan teknologi yang memiliki sumber daya dan keahlian dalam mengembangkan sistem keamanan digital. Dengan bekerja sama dengan pemerintah, mereka dapat membantu menciptakan sistem perlindungan yang lebih efektif bagi pengguna internet. Kolaborasi semacam ini dapat memperkuat upaya pencegahan terhadap berbagai bentuk kejahatan siber (Mishra, 2023).

Laporan dari masyarakat dapat membantu pihak berwenang dalam mengidentifikasi pola serangan serta melacak pelaku kejahatan. Semakin banyak laporan yang diterima, semakin mudah bagi aparat penegak hukum untuk mengungkap jaringan pelaku *phishing* yang beroperasi di dunia maya. Dalam kerangka hukum Indonesia, upaya pencegahan dan penanggulangan *phishing* didukung oleh berbagai ketentuan dalam Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik. Regulasi tersebut mengatur kewajiban pengendali data dalam melindungi informasi pribadi serta memberikan sanksi bagi pelaku penyalahgunaan data. Penegakan hukum yang konsisten terhadap pelanggaran tersebut diharapkan dapat memberikan efek jera sekaligus meningkatkan kepercayaan masyarakat terhadap keamanan ekosistem digital (Ali et al., 2024).

KESIMPULAN

Phishing merupakan salah satu bentuk kejahatan siber yang berkembang pesat seiring dengan meningkatnya penggunaan teknologi digital dalam kehidupan masyarakat. Serangan *phishing* umumnya memanfaatkan teknik rekayasa sosial yang mengeksploitasi psikologi korban agar secara tidak sadar memberikan informasi pribadi yang bersifat sensitif. Modus yang digunakan oleh pelaku juga semakin beragam dan canggih, mulai dari email *phishing*, smishing melalui pesan singkat, hingga vishing melalui panggilan telepon. Kondisi ini menunjukkan bahwa ancaman *phishing* tidak hanya berkaitan dengan aspek teknologi, tetapi juga berkaitan erat dengan perilaku dan tingkat kesadaran pengguna internet dalam menjaga keamanan data pribadi mereka. Selain itu, kerentanan manusia menjadi faktor utama yang sering dimanfaatkan oleh pelaku *phishing* untuk menjalankan aksinya. Kurangnya literasi digital, rendahnya tingkat kewaspadaan, serta kebiasaan pengguna internet yang kurang teliti dalam memeriksa sumber informasi membuat banyak individu mudah menjadi korban. Dampak yang ditimbulkan dari pencurian data pribadi juga sangat luas, mulai dari kerugian finansial, pencurian identitas, hingga gangguan psikologis bagi korban. Tidak hanya individu, organisasi dan perusahaan juga dapat mengalami kerugian besar akibat kebocoran data, baik dalam bentuk kerugian finansial, penurunan reputasi, maupun hilangnya kepercayaan dari konsumen dan masyarakat.

Dalam kajian hukum di Indonesia, upaya perlindungan terhadap data pribadi telah diatur melalui berbagai regulasi, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Kedua regulasi tersebut memberikan landasan hukum yang jelas untuk menindak pelaku kejahatan siber sekaligus melindungi hak individu atas keamanan data pribadinya. Namun demikian, efektivitas perlindungan hukum tidak hanya bergantung pada keberadaan regulasi semata, melainkan juga pada konsistensi dalam penegakan hukum serta kesadaran masyarakat dalam menjaga keamanan informasi pribadi di ruang digital. Berdasarkan kesimpulan tersebut, diperlukan berbagai upaya yang lebih komprehensif dalam mencegah dan menanggulangi kejahatan *phishing*. Pemerintah diharapkan dapat terus memperkuat kebijakan dan penegakan hukum terkait perlindungan data pribadi serta meningkatkan kerja sama dengan berbagai pihak dalam menghadapi ancaman kejahatan siber. Selain itu, organisasi dan perusahaan juga perlu meningkatkan sistem keamanan digital serta memberikan edukasi keamanan siber kepada karyawan dan pengguna layanan mereka. Di sisi lain, masyarakat sebagai pengguna internet juga perlu meningkatkan literasi digital dan selalu berhati-hati dalam membagikan informasi pribadi agar tidak mudah menjadi korban berbagai bentuk penipuan di dunia digital.

REFERENSI

Aditya, K. M. S., & Yudiantara, I. G. N. N. K. (2025). ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA PENCURIAN DATA PRIBDADI DI ERA DIGITAL. *JURNAL MEDIA AKADEMIK (JMA)*, *3*(2), 1–20.

Ali, M. M., Farhana, N., & Zaharon, M. (2024). Phishing — A Cyber Fraud : The Types , Implications and Governance. *International Journal of Education*, *33*(1), 101–121. https://doi.org/10.1177/10567879221082966

Alsubaei, F. S., & Almazroi, A. A. L. I. (2024). Enhancing Phishing Detection : A Novel Hybrid Deep Learning Framework for Cybercrime Forensics. *IEEE Access*, *12*(January), 8373–8389. https://doi.org/10.1109/ACCESS.2024.3351946

Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 , lebih dari 215 juta penduduk telah terhubung. *Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(1), 165–190.

Arif, M., Dewanto, B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan

Penambah Followers Instagram : Analisis Serangan Phising dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, *1*(4), 1–11.

Atara, I., Syallomeita, S., & Haksoro, R. A. B. (2025). ANALISIS KRIMINOLOGI TERHADAP PENCURIAN DATA PRIBADI DI ERA DIGITAL: STUDI KASUS KEBOCORAN DATA PENGGUNA APLIKASI MYPERTAMINA TAHUN 2023. *Kampus Akademik Publisher*, *3*(2), 129–140.

Baballe, M. A., Hussaini, A., Bello, M. I., & Musa, U. S. (2022). Global Journal of Research in Engineering & Computer Sciences Review Article Online Attacks Types of Data Breach and Cyber-attack Prevention Methods. *Global Journal of Research in Engineering & Computer Sciences*, *02*(05), 1–5. https://doi.org/10.5281/zenodo.7144657

Bhakti, I. D. (2025). Analisis Upaya Kejahatan Siber Terhadap Pencurian Data Digital Pengguna Internet dan Perangkat Seluler. *Prosiding Konstelasi*, *2*(1), 14–19.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2), 299. https://doi.org/10.21143/TELJ.vol2.no2.1043

Dinesh, P. M., Mukesh, M., Navaneethan, B., Sabeenian, R. S., Paramasivam, M. E., & Manjunathan, A. (2023). Identification of Phishing Machine Learning Algorithm Attacks using. *E3S Web of Conferences*, *4*(10), 1–10.

Gumay, B., Hendrawan, A. H., Satrya, F., Kusumah, F., Informatika, T., & Khaldun, U. I. (2024). ANALISIS DAMPAK ANCAMAN CYBERCRIME TERHADAP DATA MAHASISWA PADA SERANGAN WEB PHISING SIAK UIKA. *Infotech Journal*, *10*(2), 297–305.

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences (Switzerland)*, *13*(10). https://doi.org/10.3390/app13105875

Nababan, F. E., & Sumardiana, B. (2024). Kejahatan Pencurian Data Pribadi melalui Cyber Phishing dan Sistem Pembuktiannya dalam Persidangan: Studi Putusan No. 697/Pid.Sus/2024/PN.Sda. *Hukum Dan Lingkungan*, *12*(1), 627–650.

Nguyen, T. N. (2023). A review of cyber crime. *Journal of Social Review and Development*, *2*(1), 1–3.

Nyasvisvo, B., & Chigada, J. M. (2023). Phishing Attacks : A Security Challenge for University Students Studying Remotely Phishing Attacks : A Security Challenge for University Students Studying Remotely. *The African Journal of Information Systems*, *15*(2), 1–27.

Reyhan, E., & Gultom, P. (2025). PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Lex Laguens: Jurnal Kajian Hukum Dan Keadilan*, *3*(3), 111–124.

Souhoka, B. A., Fadillah, R. A., & Fathan, M. (2025). Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook. *Jurnal Sistem Informasi Galuh*, *3*(1), 10–22.

Syah, R. (2023). STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER. *Jurnal Impresi Indonesia (JII)*, *2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Trianurahmah, A., Fauzi, A., Tyas, E. N., Afif, M., Rizky, M., & Wibisono, P. (2024). Analisis Ancaman Pishing Melalui Aplikasi WhatsApp : Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Link. *Jurnal Ilmiah Multidisiplin Nusantara*, *1*(2), 60–74.

Yoro, R. E. (2023a). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and*

Computer Engineering (IJECE), *13*(2), 1922–1931. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E. (2023b). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1943–1953. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yunita, I. (2023). PENGARUH KEMAJUAN TEKNOLOGI TERHADAP PERKEMBANGAN TINDAK PIDANA CYBERCRIME (Studi Kasus Phising Sebagai Ancaman Keamanan Digital). *Jurnal Hukum Legalita*, *5*(2), 1–13.